REMARKS

Claims 2-7, 10-24, 27 and 30-32 are currently pending in the subject application.

By the present amendment, applicant has amended the specification to provide further identification of related applications, and to provide the current status of references cited; amended claims 6,10, 27 and 30; provided a clean copy of claim 12; canceled claims 25 and 26 and substituted new claim 31 therefor; and canceled claim 28 and 29 and substituted new claim 32 therefor.

In the Official Action dated August 8, 2001 the Examiner has objected to the specification and claims 2-5, 14-24, 26, 27, 29 and 30 as improperly using underlining and brackets. Applicants respectfully traverse these objections.

Applicants are not aware of any regulation that prohibits the use of underlining and brackets, which are intended to be published in the original specification and claims. Indeed prior versions of 37 CFR § 1.121, which applicants believe to have been in effect at the time the subject application was filed, explicitly provided for the use of brackets and underlining intended to be published in claims; requiring only that such claims not be amended with the use of brackets and underlining. As the present regulations both require applicants to provide a clean copy of all amended paragraphs and claims and permits the use of other markings to show changes (as applicants have done in the present amendment), there is even less reason to be concerned with the likelihood that original use of brackets and underlining intended for inclusion in the published patent will cause confusion. And, given the freedom the regulations now provide for marking up changes, to the extent such confusion is possible, it may still occur with any changed notation that applicants might substitute for the brackets and underlining used.

Applicants also note that the symbol for "point addition" , "[+]", as defined on page 5, lines 1 – 4, is used in a good faith effort to avoid confusion with the symbol for ordinary addition "+" and comply with the statutory requirement for clarity. Since both "point addition" and ordinary addition play a very significant part in the description of the embodiments of the subject invention and in the claims, use of brackets necessarily pervades the application to an extent that substitution of some other, perhaps less clear, notation would, as a practical matter, require submission of an entire new specification, as well as drawing changes to conform. In view of the heavy burden that this would impose on applicants, and the possibility of the introduction of errors in making such extensive changes, applicants respectfully submit that it is inequitable to require such changes in the absence of an explicit regulatory prohibition of the original use of brackets and underlining.

Claim 10 has been amended to delete the inadvertent indentation to which the Examiner has objected.

B

A clean version of claim 12 as originally filed has been provided by the present amendment to overcome the Examiner's objection to text in the claim that could not easily be read.

Claim 6 has been rejected under 35 USC § 112 as depending from canceled claim 1. By the present amendment claim 6 has been rewritten to depend from claim 14, which was substituted for claim 1 in the preliminary amendment dated June 9, 1999.

Claims 7, 10 – 13, 25, and 28 have been rejected under 35 USC § 102 as anticipated by U.S. patent no. 6,041,704, to: Pauschinger (hereinafter "Pauschinger").

In regard to claim 7 the Examiner states that Pauschinger teaches element b, "a certificate" at col. 5, lines 24 –29. In response, applicants note that what is actually claimed in claim 7 is an article having an imprinted indicium where the indicium comprises a certificate. There is no suggestion in Pauschinger of such indicia including certificates imprinted on articles. What Pauschinger teaches is that a "public read key" and its certificate are stored in a database (Pauschinger col. 6, lines 1 – 8) rather than being printed as part of an indicium.

The Examiner also states that Pauschinger teaches element d; which the Examiner summarizes as:

> "said private key of said first party is generated as a function of said certificate, said information, and a private key of a certifying authority"

at col. 5, lines 23 – 40. In response, applicants note that the full text of element d is:

> "said private key of said first party is generated as a function of said certificate, said information, and a private key of a certifying authority, said function being chosen so that a party wishing to verify said indicium can determine a public key corresponding to said private key of said first party by operating on said certificate and said information with a corresponding public key of said certifying authority."

Thus element d describes a particular functional relationship between a private key used to generate a signature and a certificate, where both the signature and the certificate are comprised in an indicium imprinted on an article, which is not found anywhere in Pauschinger. Rather Pauschinger teaches simply that a "private write key", corresponding to the private key of the first party, and a corresponding "public read key" are generated, apparently in any conventional manner, without regard to any certificate. (Note Pauschinger col. 5, lines 23 – 28)

Accordingly applicants respectfully submit that Pauschinger neither teaches nor suggests, whether considered alone or in combination with any of the references cited but not applied, an article imprinted with an indicium comprising such a certificate and such a signature.

B

In regard to claim 10, the Examiner states that Pauschinger discloses element a at col. 5, lines 23- 31. Element a recites:

> "a) said certifying authority providing said meter with an integer, said integer being a first function of said private key of said authority".

No teaching or suggestion of such a step where a certifying authority downloads an integer that is a function of a private key of the authority is found in Pauschinger.

The Examiner then states that Pauschinger discloses element b at col. 5, lines 23- 31. Element b recites:

> "b) said meter computing a digital postage meter private key as a second function of said integer"

while Pauschinger teaches that:

> "An asymmetrical key pair is generated, comprising a private write key Kw and a public read key Kr." (Pauschinger col. 5, lines 23 and 24)

Thus Pauschinger merely teaches that a conventional public key pair be generated in any conventional manner. Certificates are only mentioned in passing as a standard measure used to prevent use of counterfeit keys. (Pauschinger col. 5, lines 59 – 61) Nowhere does Pauschinger teach or suggest that a private key be generated as a function of an integer provided by a certifying authority where that integer is in turn a function of a private key of that authority.

With regard to element c, applicants submit that there is no mention of certifying authority publishing information, or taking any action other then providing a conventional certificate for a key pair that has been generated independently.

Element d of claim 10 recites:

> "d) said first function, said second function and said published related information are chosen so that a party seeking to verify said indicia can compute said digital postage meter public key by operating on said published related information with said published public key of said authority."

Here, as in claim 7, element d describes a particular functional relationship between a private key used to generate a signature and information, with the difference that the information is published rather than being comprised in a certificate which is a part of an indicium, which is not found anywhere in Pauschinger. Rather Pauschinger teaches simply that a "private write key", corresponding to the private key of the first party, and a

B

corresponding "public read key" are generated, apparently in any conventional manner, without regard to any published information.

Accordingly, applicants respectfully submit that Pauschinger neither teaches nor suggests, whether considered alone or in combination with any of the references cited but not applied, a method for certifying a public key as described in claim 10.

Claim 11 depends from claim 10 and is believed allowable at least for the reasons set forth with respect to claim 10.

Claim 12 is similar to claim 10, differing in that the meter private key is generated by a user and downloaded to the meter rather then being generated by the meter itself, and is believed allowable at least for the reasons set forth with respect to claim 10.

Claim 13 depends from claim 12 and is believed allowable at least for the reasons set forth with respect to claim 10.

Rejected claim 25 been canceled and independent claim 31, incorporating the limits of claims 25 and 26, has been substituted for claim 26, which depended from claim 25. Claim 27 has been amended to depend from claim 31.

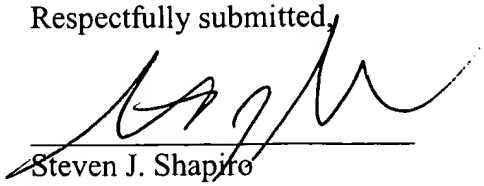
Rejected claim 28 been canceled and independent claim 32, incorporating the limits of claims 28 and 29, has been substituted for claim 29, which depended from claim 28. Claim 30, which previously depended from claim 26 and so inadvertently duplicated claim 27, has been amended to depend from claim 32.

In view of the above remarks all claims remaining in the subject application are believed to be in condition for allowance. Further consideration is requested and an early

B

allowance of all claims remaining in the subject application is respectfully solicited.

Respectfully submitted,



Steven J. Shapiro
Reg. No. 35,677
Attorney of Record
Telephone (203) 924-3880

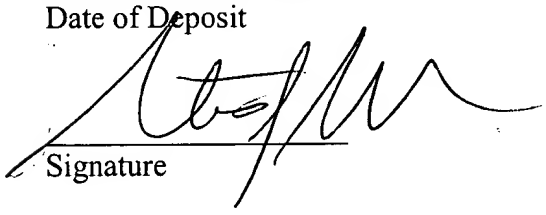
PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Assistant Commissioner for Patents
Washington, D.C. 20231

On November 8, 2001
Date of Deposit



Signature

Steven J. Shapiro
Name of Registered Rep.
Reg. No. 35,677

November 8, 2001
Date

B

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the specification:

Page 1, line 4:

--The present application is related to, and discloses subject matter common to commonly assigned, co-pending applications serial number: ~~_____~~ 09/280, 527 and 09/280,529 , (atty. docket E – 837, E-838) filed on even date herewith.

Page 3, line 13:

--In U.S. ~~application serial~~patent no.: ~~08/133,416~~5,878,136; ~~by~~to: Kim et al.; filed Oct. 8,1993, issued: March 2, 1999, a key control system comprising generation of a first set of master keys and assigning the keys to a corresponding plurality of postage meters is taught. Keys may be changed by entry of a second key via encryption with a first key.--

Page 3, line 18:

--In U.S. ~~application serial~~patent no.: ~~08/772,739~~5,661,803; ~~by~~to: Cordery et al.; ~~filed Dec. 23,1996~~issued: August 26, 1997, a method for controlling keys used in the verification of encoded information generated by a transaction evidencing device and printed on a document is taught.--

In the claims:

6. (twice amended) A method as described in claim ~~1~~ 14 wherein said message M includes information tying said postage meter's public key Key_{DM}*P to said information IAV.

10. (amended) A method for certification by a certifying authority of a public key of a digital postage meter, said digital postage meter producing indicia signed with a corresponding private key of said digital postage meter, said certifying authority having a published public key and a corresponding private key, said method comprising the steps of:

a) said certifying authority providing said meter with an integer, said integer being a first function of said private key of said authority;

b) said meter computing a digital postage meter private key as a second function of said integer; and

c) said certifying authority publishing related information; wherein

B

d) said first function, said second function and said published related information are chosen so that a party seeking to verify said indicia can compute said digital postage meter public key by operating on said published related information with ~~———~~said published public key of said authority.

27. (amended) A method as described in claim ~~26~~ 31 wherein M = (e,IAV), where IAV is an identity and attributes value for said postage meter.

30. (amended) A method as described in claim ~~26~~ 32 wherein M = (e,IAV), where IAV is an identity and attributes value for said postage meter.

B